REMARKS

Claims 11, 13, 14, 16-19, and 22-29 are pending. The Examiner's reconsideration of the rejection in view of the remarks is respectfully requested.

Claims 11, 14, 16, 18, and 22-26 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia et al. (USPAN 2001/0050990) in view of Abbondanzio (US 2003/0188176).

Claims 11, 22, and 23 are the independent claims.

Claims 11 and 22 claim, *inter alia*, "reading, by said processor, a digital signature used to sign said signed authorized boot code; decrypting said digital signature to generate a decrypted digital signature; verifying said decrypted digital signature in accordance with said first public key" and executing "said signed authorized boot code having a verified digital signature by branching to ~~a copy of~~ said signed authorized boot code in said protected memory, said signed authorized boot code including instructions for performing a boot process for a computer device comprising said processor." Claim 23 claims, *inter alia*, "a processor comprising inline cryptography and integrity hardware for executing said signed authorized boot code, said processor in signal communication with said protected memory, said processor reading and decrypting said signed authorized boot code from the protected memory and executing said signed authorized boot code from the protected memory for booting the computing device after verifying that said digital signature contained in said signed authorized boot code is valid as decrypted in accordance with a first public key stored in said protected memory, said first public key validated by a second public key permanently stored on said processor, and branching to said signed authorized boot code in said protected memory to begin the execution."

According to an embodiment of the present application, the contents of the protected memory are decrypted into plaintext by a processor, and in the case of a digital signature, verified before executing a boot code.

The Examiner's Response to Arguments is appreciated. In reply, please consider the following in connection with the amended claims.

Sudia teaches a cryptographic system with a key escrow feature (see Abstract). Sudia teaches how to perform a desired upgrade instruction in a tamper-resistance trusted device (see paragraph [0250]). Sudia fails to teach that a processor includes inline cryptography and integrity hardware for executing boot code, wherein the digital signature is also stored in an encrypted form, essentially as claimed. For example, consider paragraph [0188] of Sudia, which teaches that a sender's certificate is verified, and that the recipient's chip will not decrypt the message without verification. That is, the certificate's of Sudia are not decrypted. Compared the claimed limitations wherein the protected memory is cryptographically protected, and the digital signature used to sign the authorized boot code is encrypted.

Abbondanzio teaches methods for remotely booting devices by remotely configuring authentication parameters instead of manually installing them on the devices to be booted (see Abstract). According to Abbondanzio, public keys are transmitted prior to encrypted boot code (see block 604, FIG. 6). Here, the server blades are first booted to the network on the basis of the public keys (for example, see block 606, FIG. 6) then subsequently, the server blade may attempt to boot an encrypted boot code image (for example, see block 609, FIG. 6). Therefore, similar to Sudia, Abbondanzio there is no decryption of keys prior to receiving an encrypted boot code.

Respectfully, the combination of Sudia and Abbondanzio fails to teach or suggest the claimed protected memory storing a boot code signed by a digital signature, wherein the processor may perform an inline decryption of both the digital signature and boot code. Therefore, the combination of Sudia and Abbondanzio fails to teach or suggest all of the limitations of Claims 11 and 22.

Not withstanding the foregoing argument, Applicants maintain that the combination of Sudia and Abbondanzio is improper because the proposed modification would render the invention of Abbondanzio unsatisfactory for its intended purpose.

The intended purpose of Abbondanzio is to provide a method to perform the execution of boot code off of the system to be booted, that is, to perform a boot to network. The proposed combination requires that the processor of *a server to be booted* locally executes a boot code.

The proposed combination is counter to the express teachings of Abbondanzio, wherein the server blade boots from either deployment server 130 or customer boot server 206 (see FIG. 2 and paragraph [0058]). Thus, the server must boot to network in order to achieve the intended purpose of the invention. Stated simply, it is the express intended purpose of Abbondanzio to perform the execution of boot code from a network location. Consider paragraph [0058], which teaches:

> In step 606, the one or more server blades 110 determined to **boot from either deployment server 130 or customer boot server 206** may boot from the appropriate device, e.g., deployment server 130, customer boot server 206. In one embodiment, the one or more server blades 110 determined to boot from either deployment server 130 or customer boot server 206 may boot from the appropriate device over a public network, e.g., campus LAN 205 (FIG. 2).

In view of the foregoing, the server blade of Abbondanzio is first booted to the network. Subsequently, the booted server blade may boot a boot code image. However, in this case, the necessary result is that the server blade is already booted (from network). Therefore, the proposed combination renders the Abbondanzio reference unsatisfactory for an intended purpose because it requires that a server blade boot from a local directory.

Claims 13, 14, 16-19 depend from Claim 11. The dependent claims are believed to be allowable for at least the reasons given for Claim 11. The Examiner's reconsideration of the rejection is respectfully requested.

Claims 17, 19, 27 and 28 have been rejected under 35 U.S.C. 103(a) as being unpatentable over Sudia in view of Morgan et al. (USPN 6,185,685). The Examiner stated essentially that the combined teachings of Sudia and Morgan teach or suggest all of the limitations of Claims 17, 19, 27 and 28.

Claims 17 and 19 depend from Claim 11. Claims 27 and 28 depend from Claim 23. The dependent claims are believed to be allowable for at least the reasons given for the respective independent claims. Reconsideration of the rejection is respectfully requested.

Claim 29 depends from Claim 23 and is believed to be allowable for at least the reasons given for Claim 23.

For the forgoing reasons, the application, including Claims 11, 13, 14, 16-19, and 22-29, is believed to be in condition for allowance. Early and favorable reconsideration of the case is respectfully requested.

Respectfully submitted,

Dated: 12 January 2012

By: /Nathaniel T. Wallace/
Nathaniel T. Wallace
Reg. No. 48,909
Attorney for Applicants

F. CHAU & ASSOCIATES, LLC
130 Woodbury Road
Woodbury, New York 11797
TEL: (516) 692-8888
FAX: (516) 692-8889